REMARKS

This application has been reviewed in light of the Office Action dated May 4, 2006. Claims 1-13 are presented for examination. Claims 1, 9 and 10, which are the independent claims, have been amended to define more clearly what Applicant regards as his invention. Support for these claim amendments can be found, *e.g.*, at paragraph 150 of the specification. Dependent Claims 2-8 and 11-13 have been amended as to matters of form, in a manner not intended or believed to narrow the scope of those claims. Favorable reconsideration is requested.

Claims 1-13 were rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent Application Publication No. 2004/0176071 ("Gehrmann"). Claims 1, 9 and 10 were rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent Application Publication No. 2004/0180657 ("Yaqub"). Claim 1-13 were rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent Application Publication No. 2004/0235450 ("Rosenberg").

It is well-established that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). Moreover, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." MPEP § 2131 (quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)) (emphasis added).

Gehrmann relates to a system in which a mobile telephone can be authenticated using a subscriber identity module (SIM) accessed through a wireless connection, such as a Bluetooth link. Gehrmann describes a secure end-to-end authentication between a subscription module and a client communications terminal (Fig. 1, 106) (*i.e.*, mobile telephone). The terminal has a Bluetooth transceiver (110) for establishing a local radio link (115) for data transmission between the terminal and a Bluetooth transceiver (104) of a server communications terminal (101). The server communications terminal includes a processing unit (105) and a subscription module (*e.g.*, SIM card) (102).

The server communications terminal may grant the client communications terminal (*i.e.*, mobile telephone) access to the services and files of the subscription module (*e.g.*, SIM card). The server communications terminal may be a mobile telephone or other personal communications equipment. Alternatively, the server communications terminal may be a special remote access device which only serves as an access server for different client communication terminals.

Thus, Gehrmann, as understood by Applicant, uses a method which allows a user to establish a communication link wirelessly between a client communications terminal (*i.e.*, mobile telephone) and a subscription module (*e.g.*, SIM card), thereby allowing the user to connect to a wireless communications network without having to physically insert the SIM card into the mobile telephone. However, nothing has been found or pointed in Gehrmann that would teach or suggest a "method for facilitating remote configuration of a radio frequency (RF) module to enable the module to complete financial transactions via RF using a financial transaction account associated with an RF

module account issuer" (emphasis added), much less such a method comprising "transmitting personalization data from the RF module account issuer to the RF module via the mobile device microprocessor to enable the RF module to complete financial transactions via RF ... wherein the personalization data comprises financial transaction account data and an encryption key, the account data comprising an account number and an account expiration date", as recited in Claim 1 (emphasis added). Generally speaking, the present invention relates to a method which allows a user to configure an RF module to enable the module to complete financial transactions.

Therefore, Applicant believes that Gehrmann does not disclose, or even suggest, each and every element as set forth in Claim 1, and accordingly, Applicant submits that Claim 1 is patentable over Gehrmann.

Yaqub relates to a system and method for allowing mobile devices to simultaneously access a Subscriber Identity Module (SIM). The SIM contains a wireless transceiver, and the SIM may be located within a mobile phone, or it may be a stand-alone device. The mobile devices use a wireless protocol, such as Bluetooth, to retrieve identification information from the SIM. The devices then use this identification information to connect to a wireless communications network, such as a wireless local area network. However, as with Gehrmann, nothing has been found or pointed in Yaqub that would teach or suggest a "method for facilitating remote configuration of a radio frequency (RF) module to enable the module to complete financial transactions via RF using a financial transaction account associated with an RF module account issuer" (emphasis added), much less such a method comprising "transmitting personalization data from the RF module account issuer to the RF module via the mobile device microprocessor to

enable the RF module to complete financial transactions via RF ... wherein the personalization data comprises financial transaction account data and an encryption key, the account data comprising an account number and an account expiration date", as recited in Claim 1 (emphasis added).

Therefore, Applicant believes that Yaqub does not disclose, or even suggest, each and every element as set forth in Claim 1, and accordingly, Applicant submits that Claim 1 is patentable over Yaqub.

Rosenberg relates to a mobile communication device with security mechanisms for enabling wireless personal information transfer with increased security. In one embodiment of the invention, a smartlink module, which includes a processing chip and antennae, is provided to be coupled to a mobile communication device for providing the mobile communication device with the ability to transmit and receive wireless smartcard communications to other smartcard enabled devices. *See* Rosenberg paragraph 14. However, Rosenberg does not teach or suggest a "method for facilitating remote configuration of a radio frequency (RF) module to enable the module to complete financial transactions via RF using a financial transaction account associated with an RF module account issuer, the method comprising ... transmitting personalization data from the RF module account issuer to the RF module via the mobile device microprocessor to enable the RF module to complete financial transactions via RF ... wherein the personalization data comprises financial transaction account data and an encryption key, the account data comprising an account number and an account expiration date," as recited in Claim 1 (emphasis added).

In one embodiment of Rosenberg's apparatus, as understood by Applicant, a processing chip converts data received in the form of radio waves by one of the antennae to data in the form of digital/analog signals that are then provided to a mobile communication device through communication path and connection pin. Further, the processing chip converts from data in the form of digital/analog signals that are received from the mobile communication device through communication path and connection pin to the form of radio waves provided to the antennae that will be transmitted by one of the antennae. *See* Rosenberg paragraph 43. Elsewhere, Rosenberg states that in order to use the smartlink module with a mobile communication device, the combination of the smartlink module and mobile communication device must be initialized. *See* Rosenberg paragraph 50. During initialization, an initialization program within the processing chip of the smartlink module is activated. *See* Rosenberg paragraph 51. The initialization program provides the processor of the mobile communication device with an application from the smartlink module that includes two pieces of information, *i.e.*, the address of the location from which to download information and information on how to access a cellularly connected or internet connected server located at a unique mobile IP address. The second piece of information is the unique identification of the smartlink module, and possibly, the user's financial transaction information. *See* Rosenberg paragraph 52. The mobile communication device then initiates a call to the user's financial institution, *e.g.*, a bank, and provides the bank the two pieces of information along with the unique identification of the mobile communication device. *See* Rosenberg paragraph 52. The mobile communication device then receives from the bank several pieces of data including, the

user's name, address, phone and other information about the user, which are stored in the mobile communication device. *See* Rosenberg paragraph 52 (emphasis added).

During initialization of the smartlink module and mobile communication device according to Rosenberg, identifying information of the mobile communication device, *e.g.*, the electronic serial number (ESN) or manufacturer serial number is stored in the smartlink module. *See* Rosenberg paragraph 54. However, nothing has been found or pointed in Rosenberg that would teach or suggest the transmission of "a personalization data from the RF module account issuer to the RF module via the mobile device microprocessor to enable the RF module to complete financial transactions via RF ... wherein the personalization data comprises financial transaction account data and an encryption key, the account data comprising an account number and an account expiration date," as recited in Claim 1 (emphasis added).

The significance of an encryption key in the present invention is described in the specification of the present invention (*see* paragraphs 133-136). Generally, in order for an RFID reader according to the present invention to authenticate an RF module, the RFID reader provides to the RF module an interrogation signal which includes a random number as a part of the authentication code. Once the RF module receives the authentication code, it retrieves an encryption key from its database, encrypts the authentication code using the retrieved encryption key, and provides the encrypted authentication code to the RFID reader for verification. Once the encrypted authentication code is verified, the RF module is authenticated.[1]

[1] The claim scope of course is not limited by the details of this or other particular embodiments.

Rosenberg does not disclose an encryption key as described in the present invention or anything equivalent thereto. *A fortiori*, Rosenberg does not disclose the provision of a personalization data, which comprises financial transaction account data and an encryption key, to the RF module via the mobile device microprocessor. Therefore, Applicant believes that each and every element as set forth in Claim 1 is not found in Rosenberg and accordingly, Applicant submits that Claim 1 is patentable over Rosenberg.

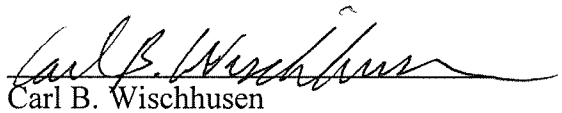
Independent Claims 9 and 10 recite features similar to those discussed above with respect to Claim 1 and are therefore also believed to be patentable over Gehrmann, Yaqub and Rosenberg for the reasons discussed above.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and early passage to issue of the present application.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,



Carl B. Wischhusen
Attorney for Applicant
Registration No. 43,279

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_Main 600594_1